

# МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра информационной безопасности



УТВЕРЖДАЮ

Проректор по учебной работе

О.Г. Локтионова

2016 г.

## ЛАБОРАТОРНАЯ РАБОТА № 5

«Исследование беспроводной сети WiFi под управлением ОС  
Linux»

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Администрирование вычислительных систем», «Администрирование вычислительных сетей» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01.

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Локтионова Оксана Геннадьевна

Должность: проректор по учебной работе

Дата подписания: 08.09.2021 16:47:09

Уникальный программный ключ:

0b817ca911e6668abb13a5d426d39e5f1c11eab073e945914a40517a56d089

Курск 2016

УДК 004

Составители: В.В. Гефнер, И.В. Калуцкий

Рецензент

Кандидат технических наук, доцент кафедры  
защиты информации и систем связи *А.Г. Сневаков*

**Исследование беспроводной сети WiFi под управлением ОС Linux:** методические указания к выполнению лабораторных и практических работ по дисциплинам: «Администрирование вычислительных систем», «Администрирование вычислительных сетей» / Юго-Зап. гос. ун-т; сост.: В.В. Гефнер, И.В. Калуцкий, Курск, 2016. 38 с.: ил. 1, Библиогр.: с. 38

Содержат сведения по вопросам возможностей беспроводной сети в ОС GNU/Linux.

Указывается порядок выполнения лабораторных и практических работ, правила оформления, содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Комплексная защита объектов информатизации», «Информационная безопасность», «Информационная безопасность автоматизированных систем».

Методические указания по выполнению лабораторных и практических работ по дисциплинам «Администрирование вычислительных систем», «Администрирование вычислительных сетей» для студентов специальностей и направлений подготовки 10.05.02, 10.05.03, 10.03.01, 10.04.01.дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . *31.05.16* Формат 60x84 1/16.

Усл. печ. л. *2,2* . Уч. –изд.л. *2,0* . Тираж 30 экз. Заказ *587* Бесплатно.

Юго-Западный государственный университет.

305040, г. Курск, ул. 50 лет Октября, 94.

## Содержание

Цель работы .....	4
Порядок выполнения работы.....	4
Содержание отчёта.....	4
Выполнение работы .....	5
Контрольные вопросы .....	14
Библиографический список .....	15

## **Цель работы**

Цель лабораторной работы – исследование беспроводной сети Wi-Fi под управлением операционной системы GNU/Linux.

## **Порядок выполнения работы**

1. Изучить теоретическую часть.
2. Выполнить задания, поставленные в данном методическом указании.
3. Сделать вывод по проделанной работе.

## **Содержание отчёта**

1. Титульный лист.
2. Задание на лабораторную работу.
3. Ход выполнения лабораторной работы со скриншотами.
4. Вывод по лабораторной работе.

## Выполнение работы

1. Изучите теоретический материал, изложенный в методических указаниях к лабораторной работе №4 «Исследование сетевых возможностей ОС Linux».

1. Загрузите операционную систему Linux с компакт-диска (Live-CD). Загрузку произведите в текстовом режиме. Зарегистрируйтесь в двух первых консолях с правами **root**, пароль администратора отображается в подсказке.

2. С помощью команды **ifconfig -a|more** проверьте доступные сетевые интерфейсы. Обратите внимание на беспроводный адаптер, обозначенный как **ath0** (или **ath1**).

```
ath0      Link encap:Ethernet  HWaddr 00:1e:58:a1:fd:bd
BROADCAST MULTICAST  MTU:1500  Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
eth0      Link encap:Ethernet  HWaddr 00:02:e3:32:db:1b
BROADCAST MULTICAST  MTU:1500  Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
```

**collisions:0 txqueuelen:1000**

**RX bytes:0 (0.0 B) TX bytes:1782 (1.7 KiB)**

**Interrupt:19**

**lo**      **Link encap:Local Loopback**                      **inet addr:127.0.0.1**  
**Mask:255.0.0.0**                      **UP LOOPBACK RUNNING**    **MTU:16436**  
**Metric:1**

**RX packets:0 errors:0 dropped:0 overruns:0 frame:0**

**TX packets:0 errors:0 dropped:0 overruns:0 carrier:0**

**collisions:0 txqueuelen:0**

**RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)**

3. Аналогично посмотрите более точную информацию о состоянии беспроводного адаптера с помощью команды **iwconfig ath0**. В каком состоянии находится этот адаптер?

**ath0**    **IEEE 802.11g ESSID:"" Nickname:""**

**Mode:Managed Channel:0 Access Point: Not-Associated**

**Bit Rate:0 kb/s Tx-Power:15 dBm Sensitivity=1/1**

**Retry:off RTS thr:off Fragment thr:off**

**Encryption key:off**

**Power Management:off**

**Link Quality=0/70 Signal level=-94 dBm Noise level=-94**

**dBm**

**Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0**

**Tx excessive retries:0 Invalid misc:0 Missed beacon:0**

4. Произведите конфигурацию виртуальных беспроводных интерфейсов. Виртуальные устройства следует создавать в заданной последовательности:

- с помощью команды **wlanconfig ath0 destroy** удалите виртуальную точку доступа,

- создайте новые виртуальные интерфейсы:

```
wlanconfig ath create wlandev wifi0 wlanmode adhoc
```

Слово **adhoc** означает, что адаптер будет работать в режиме одного из приемопередатчиков в одноранговой сети,

```
wlanconfig ath create wlandev wifi0 wlanmode monitor
```

Этот адаптер будет работать в режиме перехвата всех пакетов на заданном канале (**monitor**).

Созданные устройства автоматически получают порядковые номера **ath0** и **ath1**. Информацию об их состоянии можно получить с помощью команды **iwconfig**:

```
ath0 IEEE 802.11g ESSID:"" Nickname:""  
Mode:Ad-Hoc Channel:0 Cell: Not-Associated  
Bit Rate:0 kb/s Tx-Power:15 dBm Sensitivity=1/1  
Retry:off RTS thr:off Fragment thr:off  
Encryption key:off  
Power Management:off
```

Link Quality=0/70 Signal level=-94 dBm Noise level=-94 dBm

Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0  
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

```
ath1 IEEE 802.11g ESSID:"" Nickname:""  
Mode:Monitor Channel:0 Access Point: Not-Associated  
Bit Rate:0 kb/s Tx-Power:15 dBm Sensitivity=1/1  
Retry:off RTS thr:off Fragment thr:off  
Encryption key:off  
Power Management:off  
Link Quality=0/70 Signal level=-94 dBm Noise level=-94 dBm
```

```
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0  
Tx excessive retries:0 Invalid misc:0 Missed beacon:0
```

5. У созданных виртуальных устройств пока не установлены рабочие частоты и имя сети, а также иные параметры. Для установки некоторых параметров воспользуйтесь командой

```
iwconfig ath0 channel 1 essid "abcd"
```

После ввода команды состояние виртуального адаптера должно отображаться следующим образом:

```
ath0 IEEE 802.11g ESSID:"abcd" Nickname:""
```



Mode:Ad-Hoc      Frequency:2.412    GHz      Cell:  
02:1E:58:A1:FD:B9

Bit Rate:0 kb/s   Tx-Power:15 dBm   Sensitivity=1/1  
Retry:off   RTS thr:off   Fragment thr:off  
Encryption key:off  
Power Management:off  
Link Quality=0/70   Signal level=-93 dBm   Noise level=-93  
dBm      Rx invalid nwid:0   Rx invalid crypt:0   Rx invalid frag:0  
Tx excessive retries:0   Invalid misc:0   Missed beacon:0

6. Следующим шагом будет задание IP-адресов. Для этого используйте уже испытанную утилиту **ifconfig**:

```
ifconfig ath0 192.168.0.1 ifconfig ath1 up
```

Монитору нет необходимости иметь сетевой адрес, но активизировать его нужно. Результат, выведенный командой **ifconfig -a** после ввода параметров, отображается следующим образом:

```
ath0    Link encap:Ethernet   HWaddr 00:1e:58:a1:fd:bd  
        inet          addr:192.168.0.1          Bcast:192.168.0.255  
Mask:255.255.255.0  
  
        UP BROADCAST RUNNING MULTICAST   MTU:1500  
Metric:1  
  
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
        collisions:0 txqueuelen:0
```

**RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)**

**ath1 Link encap:UNSPEC HWaddr 06-1E-58-A1-FD-BD-  
00-00-00-00-00-00-00-  
00-00-00**

**inet addr:192.168.0.1 Bcast:192.168.0.255  
Mask:255.255.255.0**

**UP BROADCAST RUNNING MULTICAST MTU:1500  
Metric:1**

**RX packets:2011 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0**

**RX bytes:295763 (288.8 KiB) TX bytes:0 (0.0 B)**

**lo Link encap:Local Loopback inet addr:127.0.0.1  
Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:16436  
Metric:1**

**RX packets:8 errors:0 dropped:0 overruns:0 frame:0  
TX packets:8 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0**

**RX bytes:632 (632.0 B) TX bytes:632 (632.0 B)**

7. Теперь попытайтесь проверить сетевую активность иных беспроводных устройств в локальной сети. Для этого рекомендуется воспользоваться командой

**iwlist ath1 scan**

Методом проб и ошибок нетрудно убедиться, что в режиме сканирования

радиодиапазона может работать либо монитор, либо одноранговая точка. Заставить работать в данном режиме виртуальную точку доступа не удастся. Результаты выполнения команды **iwlist** могут быть такими:

**ath1 Scan completed :**

**Cell 01 - Address: 02:1E:58:A1:FD:B9**

**ESSID:"abcd"**

**Mode:Ad-Hoc**

**Frequency:2.412 GHz (Channel 1)**

**Quality=50/70 Signal level=-45 dBm Noise level=-**

**95 dBm**

**Encryption key:off**

**Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s**

**11 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s**

**48 Mb/s; 54 Mb/s**

**Extra:bcn\_int=100**

**Ex-**

**tra:wme\_ie=dd180050f2020101830002a3400027a4000042435e00  
62322f00**

**Cell 02 - Address: 06:1E:58:A1:FD:B9**

**ESSID:"abcd"**

**Mode:Master**

Frequency:2.412 GHz (Channel 1)

Quality=53/70 Signal level=-42 dBm Noise level=-95 dBm

Encryption key:off

Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s  
9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s  
48 Mb/s; 54 Mb/s

Extra:bcn\_int=100 Ex-

tra:wme\_ie=dd180050f2020101830002a3400027a4000042435e00  
62322f00

Extra:ath\_ie=dd0900037f01010024ff7f

8. Следующей тактической задачей является перехват заголовков пакетов, для чего можно использовать утилиту **tcpdump**. При отсутствии внешней сетевой активности ее можно создать с помощью команды **ping**, адресованной в один из внешних или внутренних IP-адресов.

```
tcpdump -i ath1 -xx -vv -c 5
```

9. Произведите разбор данных, выведенных в заголовке и шестнадцатеричном дампе команды **tcpdump**.

10. Отключите WEP-ключ шифрования для двух виртуальных точек **adhoc**. Для этого используйте команду

```
iwconfig ath0 key off
```

11. Подготовьте передачу незашифрованного трафика между двумя точками в одноранговой сети. Для этого наберите соответствующие команды:

- на клиентском (приемном) узле **nc -l -p 2222 > /dev/null** , чтобы не записывать ненужную информацию на диск.
- на серверном (передающем) узле **tar -czvt /etc/\* |nc -w 2 192.168.0.1 2222**

Разберитесь с синтаксисом и смыслом введенных команд.

12. На виртуальном мониторе запустите команду **tcpdump** в режиме перехвата содержимого передаваемых пакетов. После этого запустить процесс передачи незашифрованных данных вначале на клиентском, а затем на серверном узле. По информации, выводимой анализатором пакетов, убедитесь в перехвате открытой информации.

13. Произведите настройку криптоалгоритма WEP на клиентском и серверном узлах. Для этого воспользуйтесь командой

**iwconfig ath0 key 0123-4567-89AB-CDEF**

14. Повторите передачу, прием и перехват зашифрованных данных.

15. С помощью утилиты **airdump-ng**, задавая номер канала, имя файла для выводной информации и адрес узла, произведите взлом WEP– пароля. В зависимости от выбранного пароля требуется перехватить не менее 100 Мб данных.

16. Сделайте выводы относительно надежности используемого механизма шифрования.

## Контрольные вопросы

1. В каких режимах может работать беспроводный сетевой адаптер?
2. В чем состоит функциональное назначение точки доступа?
3. В чем заключаются преимущества и недостатки беспроводной одноранговой сети?
4. Как можно получить параметры открытой беспроводной сети?
5. Какими командами устанавливаются параметры беспроводного сетевого интерфейса?
6. В чем заключается процесс «взлома» криптозащиты беспроводной локальной сети?
7. Каким образом можно перехватить и отобразить данные, передаваемые в беспроводной локальной сети?

## Библиографический список

1. Техническая электронная документация по операционной системе Linux.
2. Береснев А.Л. Администрирование GNU/Linux с нуля./А.Л. Береснев –СПб.: БВХ-Петербург, 2010 – 576 с.
3. Блум, Ричард, Бреснахэн, Кристина. Командная строка Linux и сценарии оболочки. Библия пользователя/ Ричард Блум, Кристина Бреснахэн -М. : ООО “И.Д. Вильямс”, 2012. — 784 с.
4. В.В. Бакланов     Защитные механизмы операционной системы Linux: учебное пособие / В.В. Бакланов. под ред. Н.А. Гайдамакина. Екатеринбург: УрФУ, 2011. 354 с.